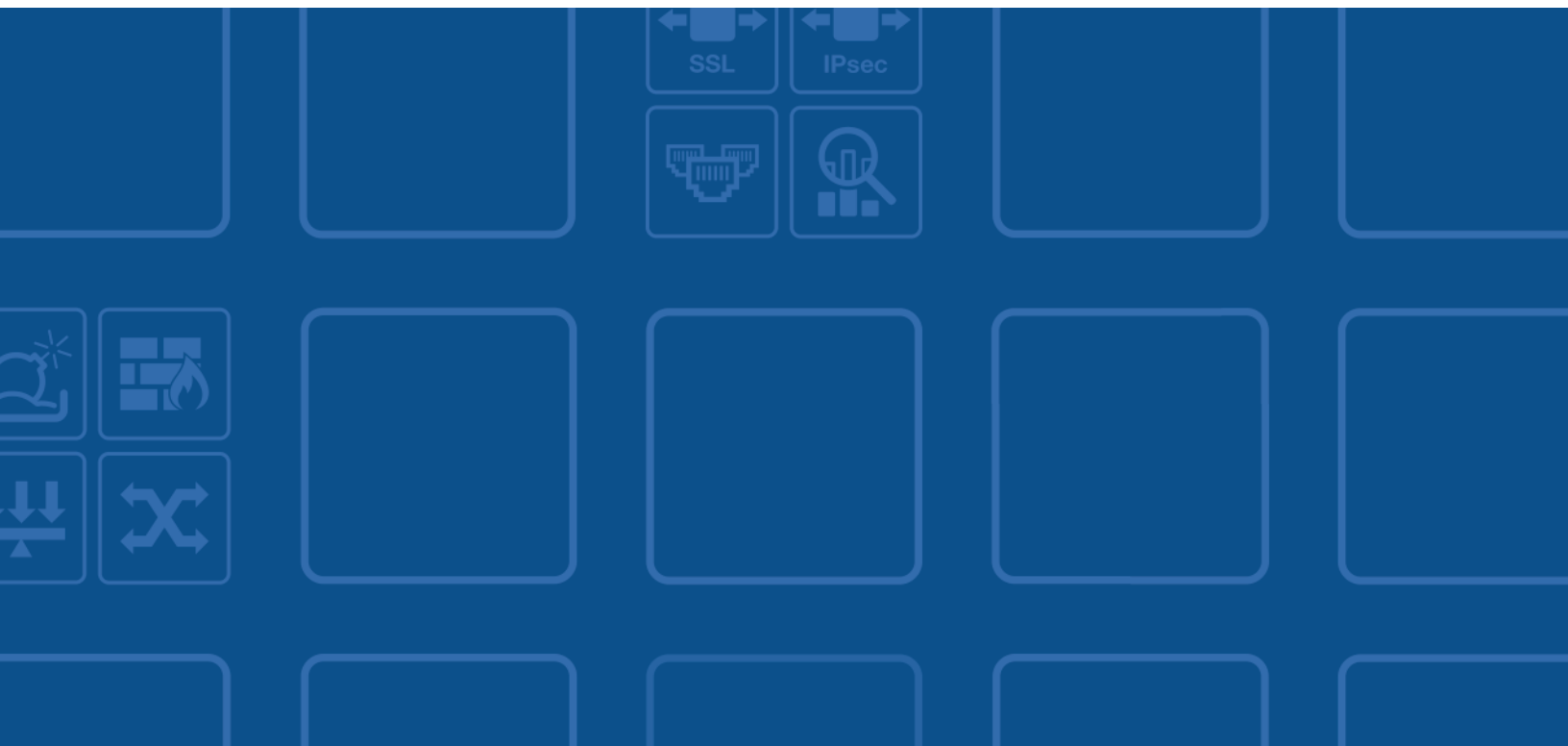
FORTINET
High Performance Network Security

FortiClient EMS - QuickStart Guide

VERSION 1.0.4



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

March 10, 2017

FortiClient Enterprise Management Server 1.0.4 QuickStart Guide

04-104-253016-20170310

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-03-10	Initial release of 1.0.4.

Introduction

This guide describes how to install and set up FortiClient Enterprise Management Server (EMS) for the first time. FortiClient EMS is used to deploy and manage FortiClient endpoints.

An informative video introducing you to FortiClient EMS is available in the Fortinet Video Library.

Supported installation platforms

You can install FortiClient EMS on the following platforms:

- Microsoft Windows Server 2012, 2012 R2
- Microsoft Windows Server 2008 R2

For information about minimum system requirements and the latest information about supported platforms, see the *FortiClient EMS Release Notes*, available in the Fortinet Document Library.

Required services and ports

You must ensure that required ports and services are enabled on the server for use by FortiClient Enterprise Management Server and its associated applications. The required ports and services enable FortiClient Enterprise Management Server to communicate with clients and servers running associated applications.

Communication	Service	Protocol	Port
FortiClient endpoint	File transfers	TCP	8013 (default)
Computer browser service • Computer browser service is not needed if an Active Directory is used or clients can manually register to EMS.	Enabled		
Samba (SMB) service • During FortiClient deployment, endpoints may connect to the FortiClient EMS server using the SMB service.	Enabled		445

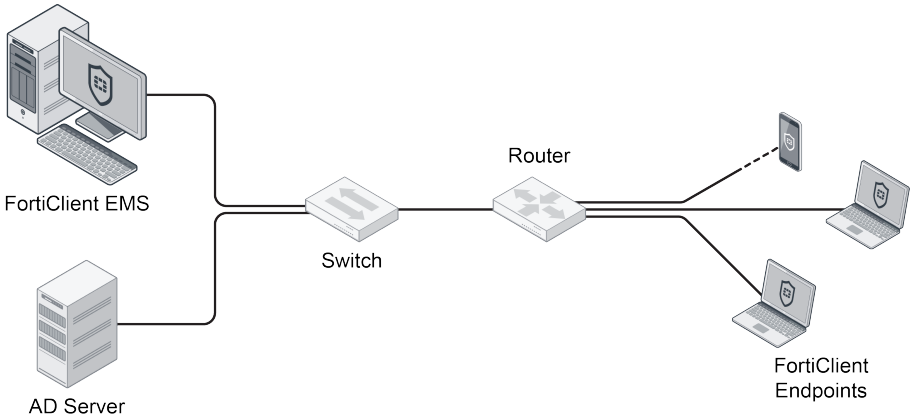
Communication	Service	Protocol	Port
Distributed Computing Environment / Remote Procedure Calls (DCE- RPC) • The FortiClient EMS server connects to the endpoints using RPC for FortiClient deployment.	Enabled		135
Active Directory server connection	When used as a default connection		389
Apache	HTTPS	TCP	443
SQL server			

Ensure that the Computer Browser Service is running. On Windows Server 2012 R2, the service is disabled by default. If this service is not active, FortiClient EMS cannot detect computers on the same network, even if they are available.

Deployment options

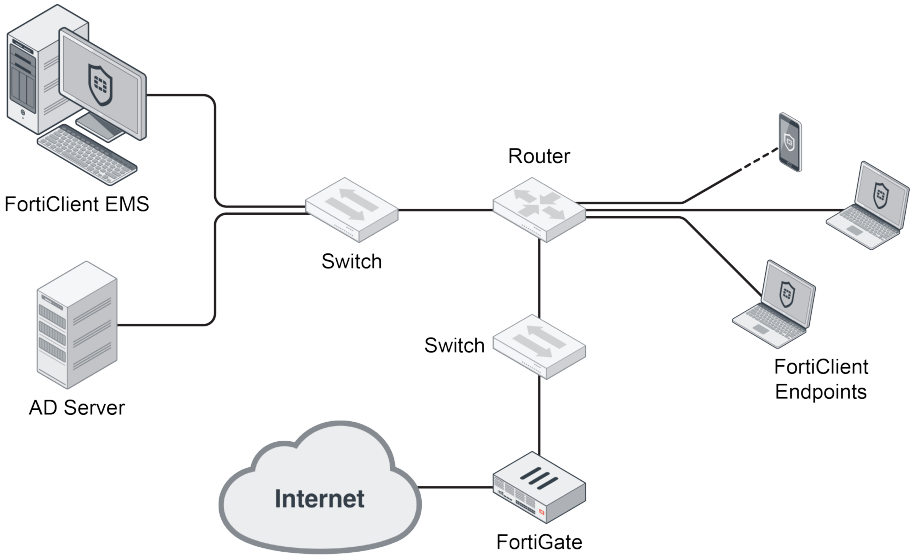
The following deployment options for EMS are supported: standalone or Integrated FortiGate.

Standalone



In standalone mode, a FortiGate device is not required, and network access compliance (NAC) is not supported. In a standalone mode, EMS deploys FortiClient software on endpoints, and FortiClient endpoints connect FortiClient Telemetry to EMS to receive configuration information from EMS. EMS is used to deploy, configure, and monitor FortiClient endpoints.

Integrated FortiGate



In integrated mode, a FortiGate device is required, and NAC is supported. In integrated mode, EMS deploys FortiClient software on endpoints, and FortiClient endpoints connect FortiClient Telemetry to FortiGate. FortiClient endpoints also connect to EMS for real-time monitoring. After FortiClient endpoints are connected, a

FortiClient profile with compliance rules is downloaded from FortiGate to the endpoint. Depending on the settings in the FortiClient profile from FortiGate, a profile of FortiClient configuration information might also be downloaded from EMS to endpoints. FortiClient endpoints are now managed, and NAC is enforced.

FortiClient uses the compliance rules from FortiGate to communicate whether the endpoint is compliant. If an endpoint fails to meet the compliance rules, the steps required to remain compliant are communicated. For more information, see the *FortiClient Administration Guide*.

Installation

For full network protection, FortiClient EMS should be installed on a server with FortiClient installed on all of your endpoint devices.

Following is a summary of how to install and start FortiClient EMS:

1. Download the installation file. See Downloading the installation file on page 9.
2. Install FortiClient EMS. See Installing FortiClient EMS on page 9.
3. Start FortiClient EMS. See Starting FortiClient EMS on page 10.

For information about upgrading FortiClient EMS, see the *FortiClient EMS Release Notes*.

An instructional video on how to install, login, and change your administrator password is available in the Fortinet Video Library.

Downloading the installation file

FortiClient EMS is available for download from the following locations:

- Fortinet Support website: https://support.fortinet.com/
- Sales representative

The following installation file is available for FortiClient EMS:

- `FortiClientEnterpriseManagement_1.0.4.<build>_x64.exe`

For more information about obtaining FortiClient EMS, contact your Fortinet reseller.

Installing FortiClient EMS

The FortiClient EMS installation package includes:

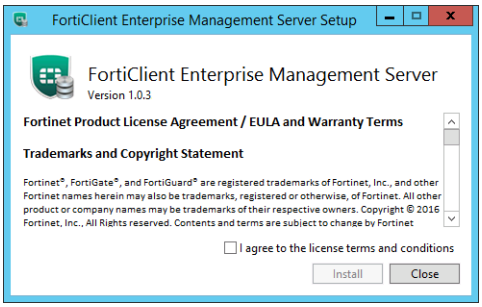
- FortiClient EMS
- Microsoft SQL Server 2014 Express Edition
- Apache HTTP server

Local administrator rights and Internet access are required to install FortiClient EMS.

To install FortiClient EMS:

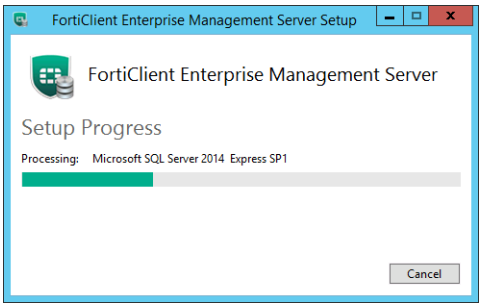
1. If you are logged into the system as an administrator, double-click the downloaded installation file.
   If you are not logged in as an administrator, right-click on the installation file, and select *Run as administrator* from the pop-up menu.

2. If applicable, select *Yes* in the *User Account Control* window to allow the program to make changes to your system.
3. In the installation window, select *I agree to the license terms and conditions*, if you agree with the license terms and conditions. If you do not agree, you cannot install the software.

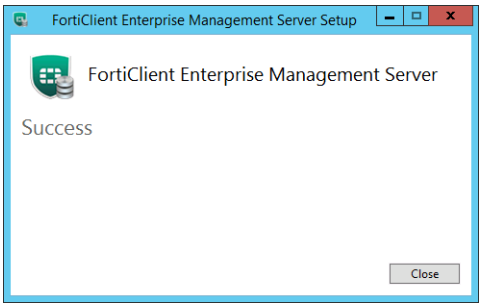


4. Select *Install*.

   The installation may take 30 minutes or longer. It may appear to stop at times, but this is only because certain steps in the installation process take longer than others. Please be patient.



5. When the program has installed correctly, the *Success* window will be displayed. Select *Close* to close the window.



   A *FortiClient Enterprise Management Server* icon will be added to the desktop.

Starting FortiClient EMS

To start FortiClient EMS:

1. Double-click the *FortiClient Enterprise Management Server* icon to start FortiClient EMS.
2. Sign in with username *admin* and no password.
3. Change the username and password by going to *View* > *User Management* > *Administration*.

4. Configure the endpoint server and client settings, including the IP address that FortiClient EMS will listen on, by going to *View* > *Settings*.

Accessing FortiClient EMS remotely

You can access FortiClient EMS remotely by using a web browser instead of the GUI.

To enable remote access to FortiClient EMS:

1. Go to *View* > *Settings*.
2. On the *Server Settings* tab, enable *Remote Administration HTTPS Access*.
3. Select *Save*.

To remotely access FortiClient EMS:

- To access EMS from the EMS server, visit `https://localhost`
- To access the server remotely, use the server's hostname: `https://<server_name>`
  Ensure that you can ping `<server_name>` remotely. This can be achieved by adding it into a DNS entry or by adding it to the Windows hosts file. You may have to modify the Windows firewall rules to allow the connection.

Endpoint Management Setup

This section describes how to set up FortiClient EMS for endpoint management. Following is a summary of how to set up endpoints:

1. Configure user accounts. See Configuring user accounts on page 12.
2. Discover endpoints by adding domains and/or discovering local endpoints. See Discovering endpoints on page 13
3. Create FortiClient Telemetry Gateway IP Lists. See Creating FortiClient Telemetry Gateway IP Lists on page 14.
4. Assign the lists to domains or workgroups. See Assigning FortiClient Telemetry Gateway IP Lists on page 14.

   Alternately, you can add a FortiClient Telemetry Gateway IP List to a custom FortiClient installer by using the FortiClient Configurator tool.
5. Add a FortiClient installer to EMS. See Adding FortiClient installers on page 15.
6. Create an endpoint profile and select a FortiClient installer. See Adding endpoint profiles on page 16.
7. Apply a profile to a workgroup or domain, an endpoint group, or an organizational group. See Assigning endpoint profiles on page 19.

   Depending on the configuration of the selected profile, FortiClient will be installed on the endpoints to which the profile is applied.

   After FortiClient installation, the endpoint user must connect FortiClient Telemetry to FortiGate or FortiClient EMS to receive the profile configuration and complete the endpoint management setup. See Connecting FortiClient Telemetry to FortiClient EMS on page 19.
8. For endpoints that are managed by the EMS, select a domain or group to view the applied profile, view a list of the endpoints in that group, and run quick and full virus scans on the endpoints.

   For endpoints that are managed by a FortiGate device, no scanning is done via the EMS.

Configuring user accounts

You can configure users to have no access to FortiClient EMS, or you can configure users to have administrator access to FortiClient EMS. You can configure local Windows users, LDAP users, or both local Windows users and LDAP users.

For local Windows users, the list of users is derived from the server on which FortiClient EMS is installed. If you want to add more users, you must add them to the server.

For LDAP users, you must add an LDAP server to FortiClient EMS, and then configure users.

To add a LDAP server:

1. Go *View* > *User Management*.
2. Select the *LDAP Server* tab.
3. Configure the options, and click *Test*.
4. If the test is successful, select *Save*.

To configure users:

1. Go to *View* > *User Management*.
2. On the *Administration* tab, click *+Add* from the toolbar.
3. In the *Add User* list, select *Windows User* or *LDAP User*.
   The *LDAP User* options is available only after you add an LDAP server to FortiClient EMS.
4. Select the specific domain access for the user.
5. Configure the permissions.
6. Click *Save*.

Discovering endpoints

You can use the following methods to discover endpoints:

- Use an Active Directory (AD) server to discover endpoints
- Scan local workgroups to discover endpoints

You can add AD servers under the *Domains* heading. Workgroup computers are listed under *Other groups* in the *Endpoints* pane.

Computers using Microsoft Windows' Computer Browser Service can be discovered and added to EMS.

An instructional video on how to Add a Domain is available in the Fortinet Video Library.

Using AD servers to discover endpoints

Endpoints imported from an AD server may already have a structured organization, or containers and computers discovered from the local network may already belong to a workgroup. If you want to change these pre-existing structures, you can create custom groups in EMS by right-clicking in the *Domains* or *Workgroups* section and selecting *Create Group*. You can move endpoints or other groups into the custom groups by right clicking on them and selecting *Move to*.

To use AD servers:

1. From the *Endpoint* pane toolbar, click *Add a new domain*. The *Domain Settings* pane opens.
2. Enter the following information.

Group Name	Enter a name for the group.
Server IP/Name	Enter the AD server IP address or name.
Server Port	Select the server port.

Distinguished Name	Enter the distinguished name (optional).
	Format:
	`OU=<organizational_unit>,...,OU=<organizational_unit>,DC=<domain_name>,DC=<domain_postfix>`
	
	Example:
	`OU=Americas,OU=Spectrum,DC=Spectrum,DC=ca`

Bind Type	Select the bind type. If *Regular* is selected, enter the *User DN* and *Password*. Select whether to show the password and use the secure LDAPS connection protocol.

3. Select *Test* to test the domain settings.
4. If the test is successful, select *Save* to save the new domain.
   If the test is not successful, correct the information as required, and then test the settings again.

Scanning local workgroups to discover endpoints

To scan local workgroups:

1. Select *View* > *Settings*.
2. On the *Server Settings* tab, enable the *Scan local workgroups* option.
3. Select *Save*.

Creating FortiClient Telemetry Gateway IP Lists

The FortiClient Telemetry Gateway IP List identifies IP addresses for FortiGate and/or EMS to which endpoints can connect FortiClient Telemetry. You can create one or more FortiClient Telemetry Gateway IP Lists, and assign the list to a domain or workgroup.

To create a FortiClient Telemetry Gateway IP List:

1. Go to *FortiClient Telemetry Gateway IP List*.
2. Click the + button.
3. Configure the options, and select *Save*.

Assigning FortiClient Telemetry Gateway IP Lists

To assign FortiClient Telemetry Gateway IP Lists:

1. Right-click a domain or workgroup, select *Assign FortiClient Telemetry Gateway IP List*, and select a FortiClient Telemetry Gateway IP List.

Adding FortiClient installers

FortiClient EMS automatically connects to FortiGuard Distribution Network (FDN) to provide access to FortiClient installers that you can use with FortiClient EMS profiles. You can customize the FortiClient installers by using FortiClient EMS. If a connection to FDN is not available, you must manually download FortiClient installers to use with FortiClient EMS.

Alternately you can create custom FortiClient installers by using the FortiClient Configurator tool, and then upload the custom installers to FortiClient EMS.

The following services must be enabled and configured on each Windows endpoint before FortiClient is deployed to them:

- Task Scheduler: Automatic
- Windows Installer: Manual
- Remote Registry: Automatic

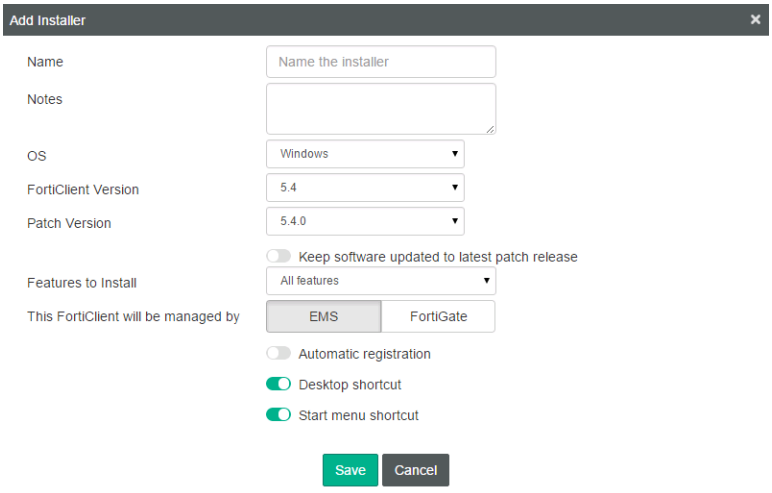
The Windows Firewall must be configured to allow the following inbound connections:

- File and Printer Sharing (SMB-In)
- Remote Scheduled Tasks Management (RPC)

For AD group deployments, an AD administrator account is required. For non-AD deployments, the installer URL can be shared with users, who can then download and install FortiClient manually.

To add an installer:

1. Select *View* > *Software Manager*. The *FortiClient Software Manager* pane opens.
2. Select *Add* to open the *Add Installer* window.



3. Configure the following settings:

Name	Enter a name for the installer.

Notes	Optionally, enter notes describing the installer.
OS	Select the OS to which the installer will apply, *Windows* or *Mac OS X*.
FortiClient Version	Select the FortiClient version that the installer will install, or select *Upload* to upload an installer file.
Patch Version	Select the patch version of FortiClient that will be installed. Select *Keep software updated to latest patch release* to force the software to automatically update to the latest patch.
Keep software updated to latest patch release	Select to keep FortiClient updated to the latest available patch release.
Features to Install	Select the features to install, one of: • *All features* • *Security only* • *VPN only* • *AntiVirus, Web Filtering, and Vulnerability Scan only* • *Web Filtering only* • *Vulnerability Scan only* • *Application Firewall only* • *Application Firewall, Web Filtering, and Vulnerability Scan* • *Application Firewall, VPN, Web Filtering, and Vulnerability Scan*
This FortiClient will be managed by	Select whether *EMS* or *FortiGate* will manage the endpoint.
Automatic Registration	Turn automatic registration on or off. When enabled, after installation FortiClient will automatically register to the first possible IP in the registration IP list.
Desktop Shortcut	Select whether or not a desktop shortcut will be created for FortiClient on the endpoint.
Start menu shortcut	Select whether or not a start menu shortcut will be created for FortiClient on the endpoint.

4. Select *Save* to create the new installer.

Adding endpoint profiles

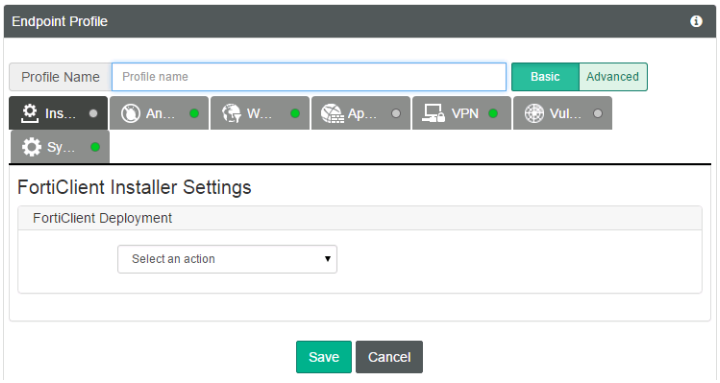
You can create endpoint profiles by using EMS, or you can import FortiClient profiles from FortiGate to EMS.

You can assign endpoint profiles to device groups or domains. If you do not apply an endpoint profile to a specific group or domain, the default endpoint profile is automatically applied.

Creating endpoint profiles

To create endpoint profiles:

1. From the *Endpoint Profiles* pane toolbar, click *Add a new profile*. The *Endpoint Profile* pane opens.
   Alternately, you can click the *Clone* icon in the default profile row to create a new endpoint profile based on the default endpoint profile.



2. Optionally, click *Advanced* to configure the endpoint profile by directly editing the XML code.
3. If using the basic configuration option, configure the following settings:

Profile Name	Enter a name for the endpoint profile, from 1 to 128 character with no special characters.
Install Options	Select a FortiClient installer to include in the endpoint profile. See Adding FortiClient installers on page 15
Feature Settings	Configure endpoint profile feature settings. See the *FortiClient EMS Administration Guide* for information about the options.
AntiVirus Protection	Enable antivirus protection, and configure the options.
Web Filtering	Enable web filtering, and configure the options.
Application Firewall	Enable application control, and configure the options.
VPN	Enable VPN use, and configure the options.
Vulnerability Scan	Enable vulnerability scan, and configure the options.
System Settings	Configure the options for system settings. See the *FortiClient EMS Administration Guide* for information about the options.

4. Select *Save* to save the endpoint profile.
   After creating the endpoint profile, you can apply the endpoint profile to AD organizational units, groups, or workgroups with the right-click menu.

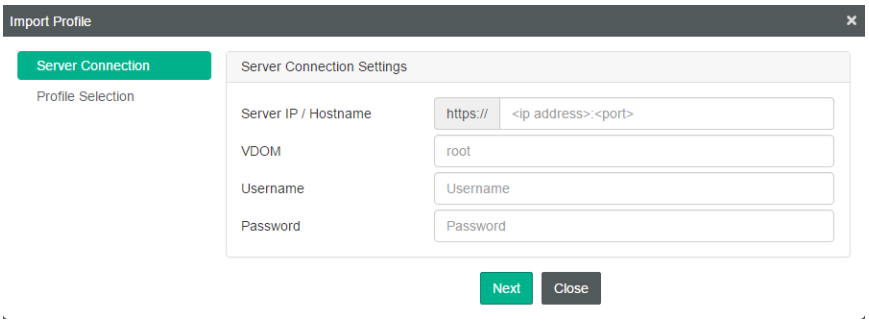
Importing FortiClient profiles from FortiGate

In FortiOS, endpoint profiles are called FortiClient profiles. You can import a FortiClient profile into EMS.

This feature requires a FortiGate running FortiOS 5.4.0 and later.

To import a FortiClient profile from FortiGate:

1. From the *Endpoint Profiles* pane toolbar, click *Import profile from FortiGate*. The *Import Profile from FortiGate* window opens.



2. Configure the following settings:

Server IP / Hostname	Enter the IP address and hostname of the FortiGate device from which the profile is being imported, in the format: `<ip address>`.
VDOM	Enter a VDOM name from the FortiGate if applicable.
Username	Enter the device' s login username.
Password	Enter the device's login password.

3. Select *Next*.
4. If a registration key has been configured, enter it in the *Registration Key* field, then select *Next*.
5. Select the FortiClient profiles from the FortiGate that will be imported to the EMS.

   The selected FortiClient profiles are automatically named and listed in the *Profile to Import* box. Selecting a FortiClient profile from the *Profile to Import* box will display a preview of the FortiClient profile, in XML, in the *Profile Preview* box.
6. Optionally, select whether to automatically synchronize the profile in EMS when you update the profile in FortiOS by enabling the *Auto-sync every* option and specifying a time interval.
7. Select *Import* to import the selected FortiClient profiles.

   The imported FortiClient profiles will be listed under the *Endpoint Profiles* pane in a group named after the FortiGate device from which they were imported.

Imported FortiClient profiles are read-only in FortiClient EMS. However, you can enable automatic synchronization of imported profiles in the profile settings. Then when you update the profile in FortiGate, the changes are automatically updated in FortiClient EMS.

8. To add an installer to the profile, select a profile to open the *Endpoint Profiles* page, then select an installer in the *Install Options* tab.

   Custom installers can also be created. See Adding FortiClient installers on page 15.

Assigning endpoint profiles

You can assign endpoint profiles to device groups or domains. If you do not apply an endpoint profile to a specific group or domain, the default endpoint profile is automatically applied.

Depending on the configuration of the selected profile, FortiClient will be installed on the endpoints to which the profile is applied.

To assign endpoint profiles:

1. Right-click on the organizational unit, group, domain, or workgroup in the *Endpoint* pane.

   You can apply profiles to groups at any level. Nested groups with unassigned profiles inherit profiles from their immediate parent group.
2. From the right-click menu, select *Assign profile*, then select the name of the profile that is to be assigned to that unit.

Connecting FortiClient Telemetry to FortiClient EMS

Endpoint users must connect FortiClient Telemetry to FortiGate or FortiClient EMS. After FortiClient Telemetry is connected, a profile is downloaded to FortiClient, and the endpoint device is managed.

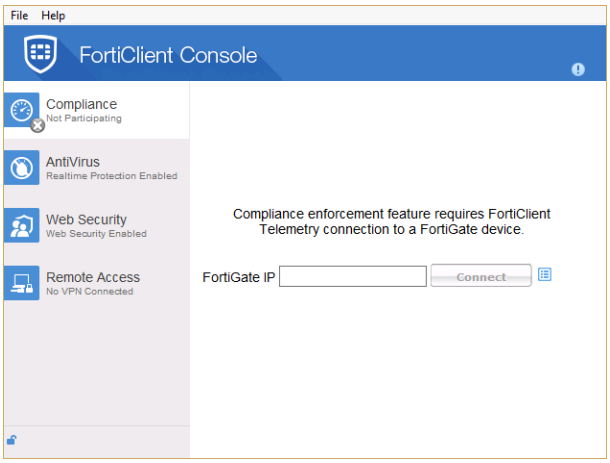
This section describes how to manually connect FortiClient Telemetry. You can configure an automatic FortiClient Telemetry connection by creating a FortiClient Telemetry Gateway IP List in FortiClient EMS, and assigning the list to one or more gateways or workgroups. Alternately, you can create a custom FortiClient installer that includes a FortiClient Telemetry Gateway IP List.

The registration terminology changed in FortiClient 5.4.1 and later. FortiClient 5.4.1 and later connects FortiClient Telemetry to FortiGate/EMS to be managed. FortiClient 5.4.0 and earlier, registers to FortiGate/EMS to be managed.

For more information about custom FortiClient installers and FortiClient Telemetry connections, see the *FortiClient Administration Guide*, available in the Fortinet Document Library.

To manually connect FortiClient Telemetry:

1. Ensure FortiClient 5.4.1 or later is installed on the endpoint device.
2. In FortiClient console, click the *Compliance* tab.



3. In the *FortiGate IP* box, type the IP address configured in FortiClient EMS, and click *Connect*.
   For information about the IP address configured in FortiClient EMS, see Starting FortiClient EMS on page 10.

   FortiClient Telemetry connects to FortiClient EMS.

FORTINET®

High Performance Network Security